

JOESandbox Cloud BASIC



ID: 539503

Sample Name: 210629

Purchase Order 449

BURGHAUSEN (uZ 20-
270)_PDF.exe

Cookbook: default.jbs

Time: 12:42:11

Date: 14/12/2021

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report 210629 Purchase Order 449 BURGHAUSEN (uZ 20-270)_PDF.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: GuLoader	3
Yara Overview	3
Memory Dumps	3
Sigma Overview	3
Jbx Signature Overview	4
AV Detection:	4
Networking:	4
System Summary:	4
Data Obfuscation:	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	7
Contacted Domains	7
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	9
Static PE Info	9
General	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	10
Code Manipulations	10
Statistics	10
System Behavior	10
Analysis Process: 210629 Purchase Order 449 BURGHAUSEN (uZ 20-270)_PDF.exe PID: 5784 Parent PID: 3568	10
General	10
File Activities	10
Registry Activities	10
Key Created	10
Key Value Created	10
Disassembly	10
Code Analysis	10

Windows Analysis Report 210629 Purchase Order 449 B...

Overview

General Information

Sample Name:	210629 Purchase Order 449 BURGHAUSEN (uZ 20-270)_PDF.exe
Analysis ID:	539503
MD5:	1547238c5f89a46.
SHA1:	b83e59cfe50f76...
SHA256:	3e6418ff545a4ca..
Tags:	exe
Infos:	
Most interesting Screenshot:	

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

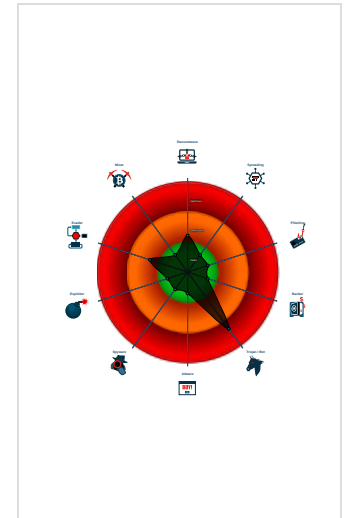
GuLoader

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm...
- Yara detected GuLoader
- Initial sample is a PE file and has a ...
- Executable has a suspicious name (...)
- C2 URLs / IPs found in malware con...
- Uses 32bit PE files
- Sample file is different than original ...
- PE file contains strange resources
- Contains functionality to read the PEB
- Uses code obfuscation techniques (...)
- Detected potential crypto function

Classification



Process Tree

- System is w10x64
- 210629 Purchase Order 449 BURGHAUSEN (uZ 20-270)_PDF.exe (PID: 5784 cmdline: "C:\Users\user\Desktop\210629 Purchase Order 449 BURGHAUSEN (uZ 20-270)_PDF.exe" MD5: 1547238C5F89A46F4F3D448138478E05)
- cleanup

Malware Configuration

Threatname: GuLoader

```
{  
  "Payload URL": "https://drive.google.com/uc?export=download&id=1sw9p"  
}
```

Yara Overview


Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.814005809.0000000004E1 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

 Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file

Networking:

- C2 URLs / IPs found in malware configuration

System Summary:

- Initial sample is a PE file and has a suspicious name
- Executable has a suspicious name (potential lure to open the executable)

Data Obfuscation:

- Yara detected GuLoader

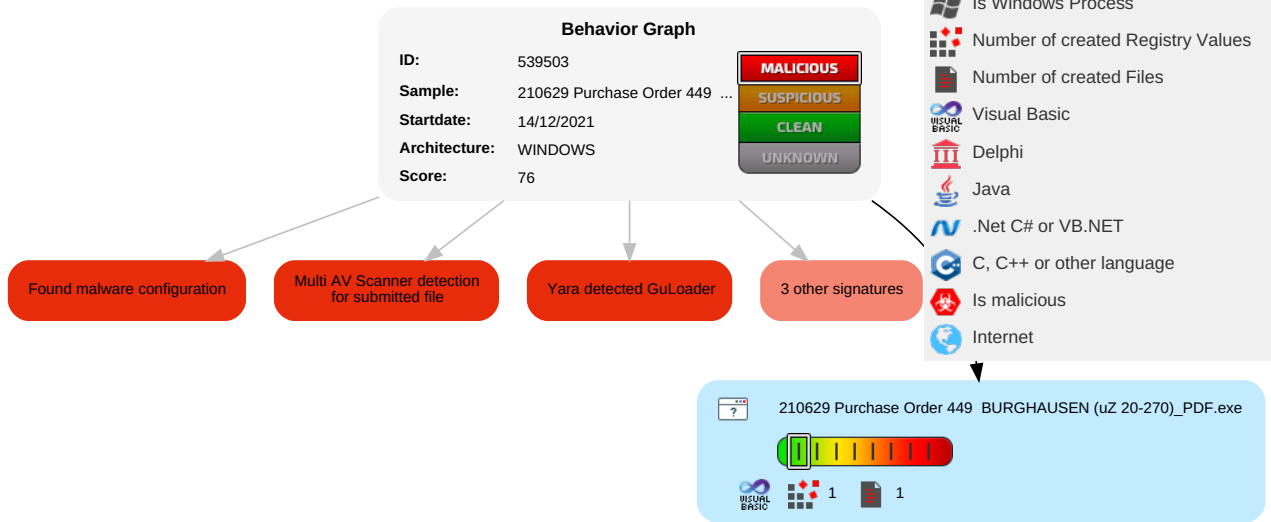
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Software Packing 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Part
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Behavior Graph

Legend:

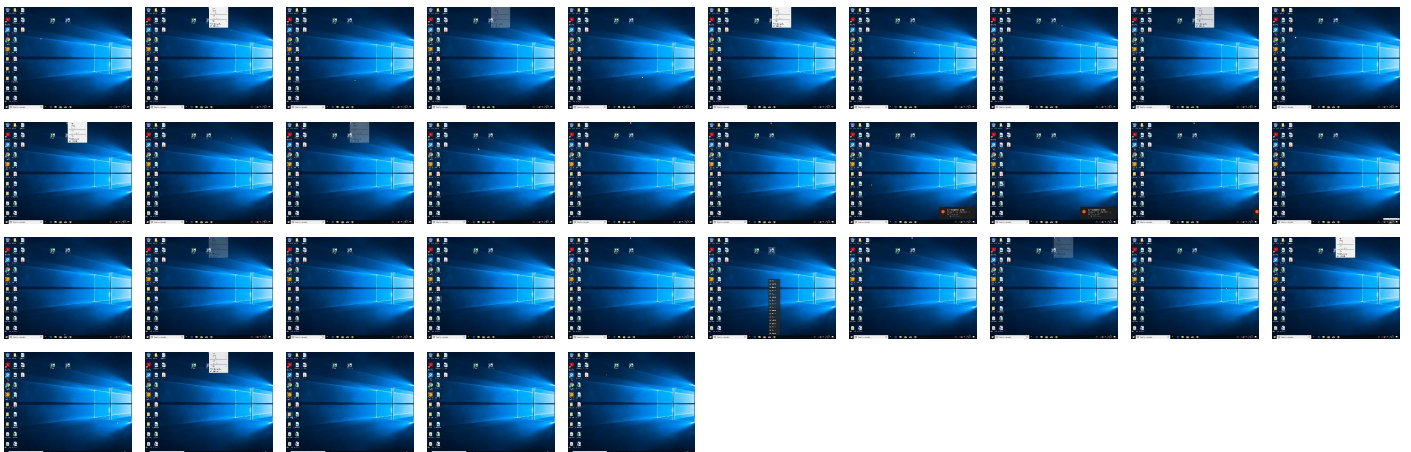
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
210629 Purchase Order 449 BURGHAUSEN (uz 20-270)_PDF.exe	34%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	539503
Start date:	14.12.2021
Start time:	12:42:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	210629 Purchase Order 449 BURGHAUSEN (uZ 20-270)_PDF.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	<ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.troj.winEXE@1/1@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 29% (good quality ratio 19.6%)• Quality average: 38%• Quality standard deviation: 32.3%
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none">• Adjust boot time• Enable AMSI• Found application associated with file extension: .exe• Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\~DF66A3895C75D2E9C9.TMP

Process:	C:\Users\user\Desktop\210629 Purchase Order 449 BURGHAUSEN (uZ 20-270)_PDF.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.9704190403390272
Encrypted:	false
SSDEEP:	24:rohKifA3iuOH/AcaVRIJ0lBeVYwqDnKolnBX26:rUKifAyxAPM03wewqDKolnB
MD5:	F8A7BA0B6BDD9C33070359F2E417C6B3
SHA1:	264F7F9354D53EF8198E0EF71962290E469BEAAF
SHA-256:	8ED5A6E47FACFC9FA4FE11F98B198F7F75A3A3F8B0A3A4C56A949E6D3D3EF13A
SHA-512:	B2A39C9F4B1E6A66A95BA8BF8E899BC9D851133E083C45203EAF1DFA1DDB83437E9A79C535B33746C358C8C100EE456A8DA227CEE9BAC360896E27D6F2D8BC4A
Malicious:	false
Reputation:	low
Preview:>.....


Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.885277653187616
TrID:	<ul style="list-style-type: none">Win32 Executable (generic) a (10002005/4) 99.15%Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81%Generic Win/DOS Executable (2004/3) 0.02%DOS Executable Generic (2002/1) 0.02%Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	210629 Purchase Order 449 BURGHAUSEN (uZ 20-270)_PDF.exe
File size:	167936
MD5:	1547238c5f89a46f4f3d448138478e05
SHA1:	b83e59cffe50f76e819731d506efd045c55aaabc

General	
SHA256:	3e6418ff545a4ca402fd68da393fd9db7ed7e798ffed1de2fbcd9bb31fa08817f
SHA512:	81b287cac12ef493bc3d8d45efcab4e268833e8365d59c2c8c9aacd849c43f3296fbc93ac4feff779f9380d0f8ddc1f73a0248ed5ff96309ff7736188a1fb2
SSDEEP:	1536:ggH9P8HOja+Zg/EsPdCFWGUbu8yljJNa+I37KTqXpzV5pkNXuUAnX:gG9P8u7ZQmeGUbuUljJNS7hXvUANX
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode...\$.x.....\.....%.....Rich.....PE..L...+.J...P.....\.....p....@

File Icon

	
Icon Hash:	93f1e0c8d2e4f9fb

Static PE Info

General	
Entrypoint:	0x40195c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4AAB2E2B [Sat Sep 12 05:14:19 2009 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	e7597de960f525af7c9e8aa5873fcec3

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x25ba0	0x26000	False	0.558214689556	data	7.13735500913	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x27000	0x36e4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2b000	0x850	0x1000	False	0.322021484375	data	3.0856399087	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ


Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
--------------------------------	----------------------------------	-----

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: 210629 Purchase Order 449 BURGHAUSEN (uZ 20-270)_PDF.exe
PID: 5784 Parent PID: 3568

General

Start time:	12:43:04
Start date:	14/12/2021
Path:	C:\Users\user\Desktop\210629 Purchase Order 449 BURGHAUSEN (uZ 20-270)_PDF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\210629 Purchase Order 449 BURGHAUSEN (uZ 20-270)_PDF.exe"
Imagebase:	0x400000
File size:	167936 bytes
MD5 hash:	1547238C5F89A46F4F3D448138478E05
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none"> Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.814005809.000000004E10000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis

